Figure 1 - GSM1x System Architecture using the MSN
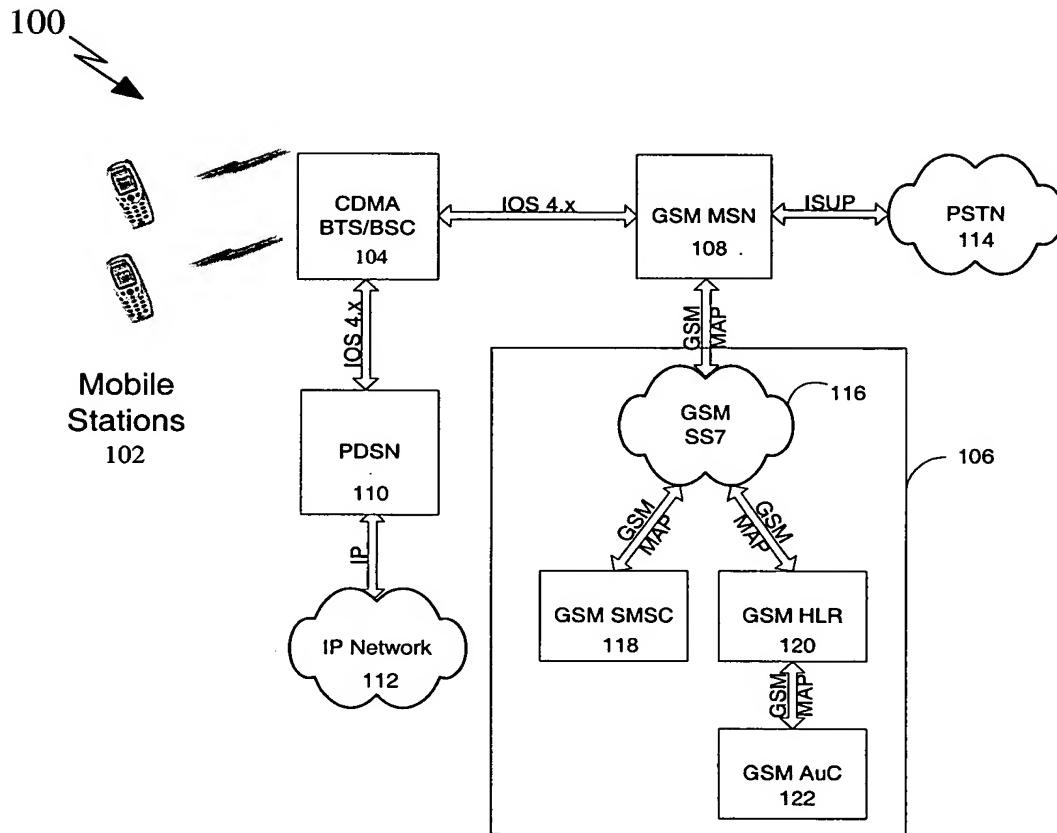

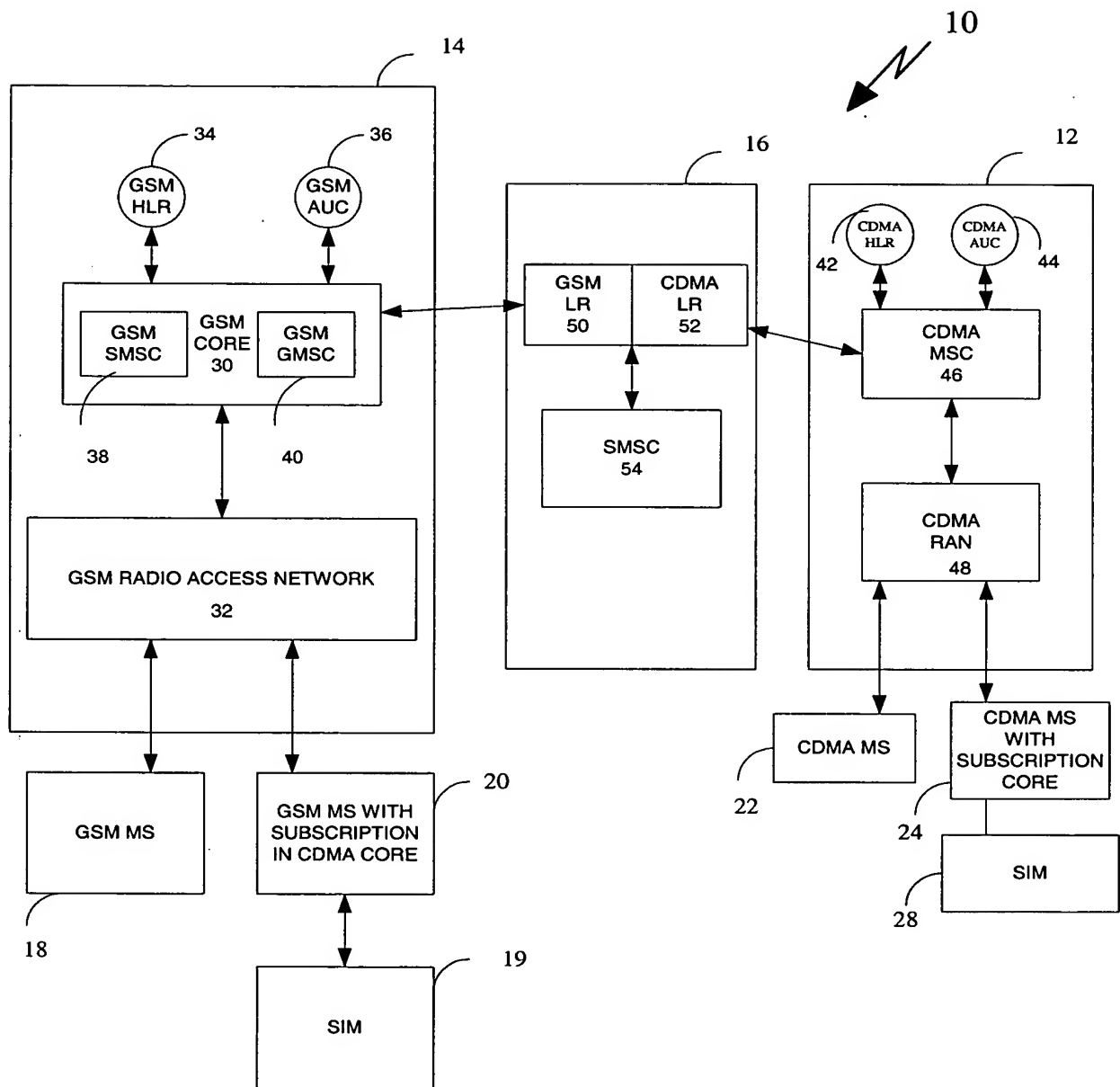FIGURE 1

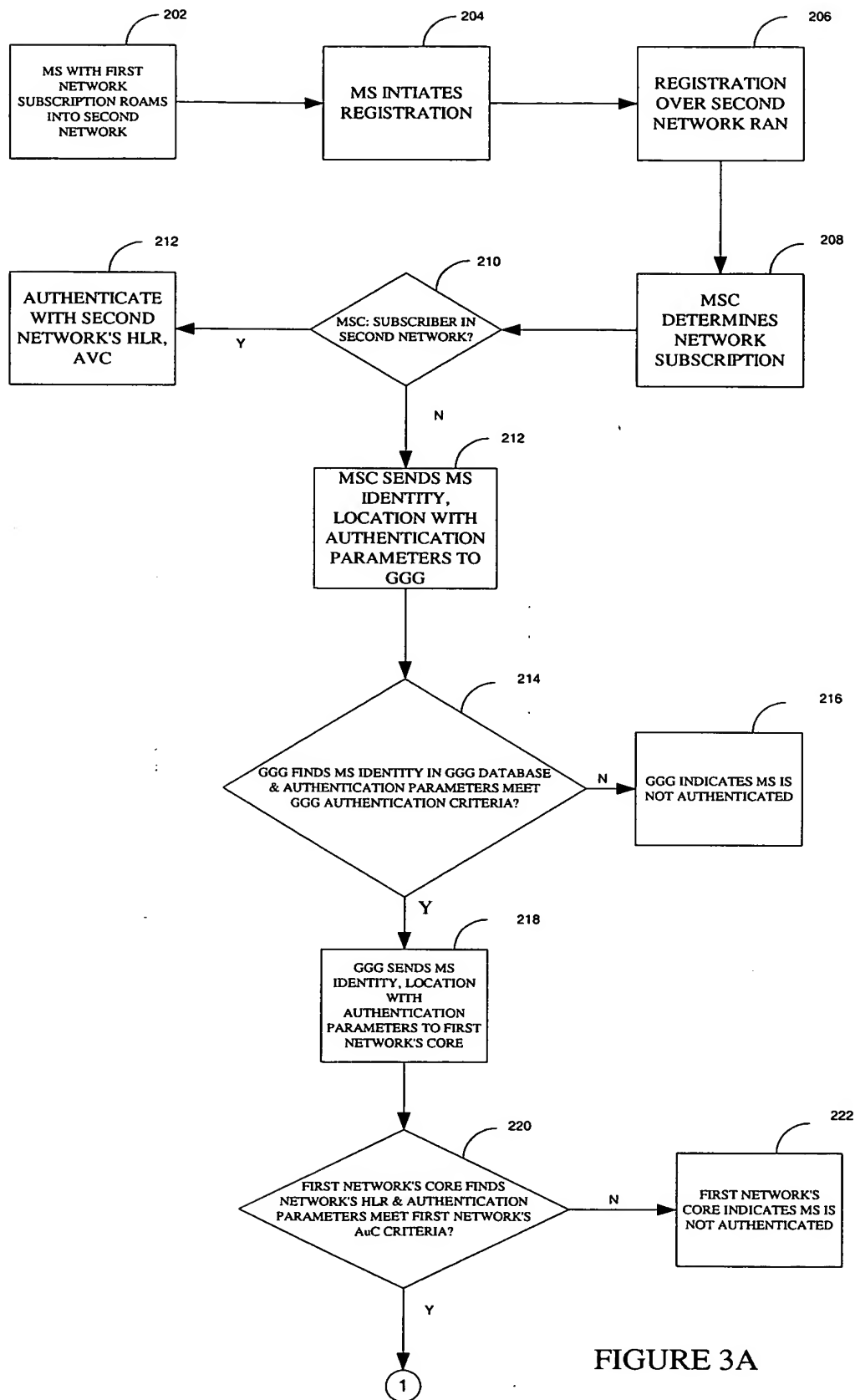FIGURE 2

```
┌──────────────┐      ┌──────────────┐      ┌──────────────┐
│ MS WITH FIRST│  202 │              │  204 │ REGISTRATION │  206
│   NETWORK    │      │ MS INTIATES  │      │ OVER SECOND  │
│ SUBSCRIPTION │ ───▶ │ REGISTRATION │ ───▶ │ NETWORK RAN  │
│ ROAMS INTO   │      │              │      │              │
│SECOND NETWORK│      │              │      │              │
└──────────────┘      └──────────────┘      └──────┬───────┘
                                                    │
                                                    ▼
┌──────────────┐  212                        ┌──────────────┐  208
│ AUTHENTICATE │                             │     MSC      │
│ WITH SECOND  │      ◇ 210                   │  DETERMINES  │
│NETWORK'S HLR,│ ◀─── MSC: SUBSCRIBER IN ◀─── │   NETWORK    │
│     AVC      │   Y   SECOND NETWORK?        │ SUBSCRIPTION │
└──────────────┘                             └──────────────┘
                          │ N
                          ▼
                  ┌──────────────┐  212
                  │ MSC SENDS MS │
                  │   IDENTITY,  │
                  │ LOCATION WITH│
                  │AUTHENTICATION│
                  │ PARAMETERS TO│
                  │     GGG      │
                  └──────┬───────┘
                         │
                         ▼
              ◇ 214                            ┌──────────────┐  216
       GGG FINDS MS IDENTITY IN GGG DATABASE   │ GGG INDICATES│
       & AUTHENTICATION PARAMETERS MEET    N   │   MS IS NOT  │
       GGG AUTHENTICATION CRITERIA?      ───▶  │ AUTHENTICATED│
                                               └──────────────┘
                         │ Y
                         ▼
                  ┌──────────────┐  218
                  │ GGG SENDS MS │
                  │   IDENTITY,  │
                  │ LOCATION WITH│
                  │AUTHENTICATION│
                  │ PARAMETERS TO│
                  │FIRST NETWORK'S│
                  │     CORE     │
                  └──────┬───────┘
                         │
                         ▼
              ◇ 220                            ┌──────────────┐  222
       FIRST NETWORK'S CORE FINDS              │FIRST NETWORK'S│
       NETWORK'S HLR & AUTHENTICATION     N    │ CORE INDICATES│
       PARAMETERS MEET FIRST NETWORK'S   ───▶  │  MS IS NOT   │
       AuC CRITERIA?                           │ AUTHENTICATED│
                                               └──────────────┘
                         │ Y
                         ▼
                        (1)
```
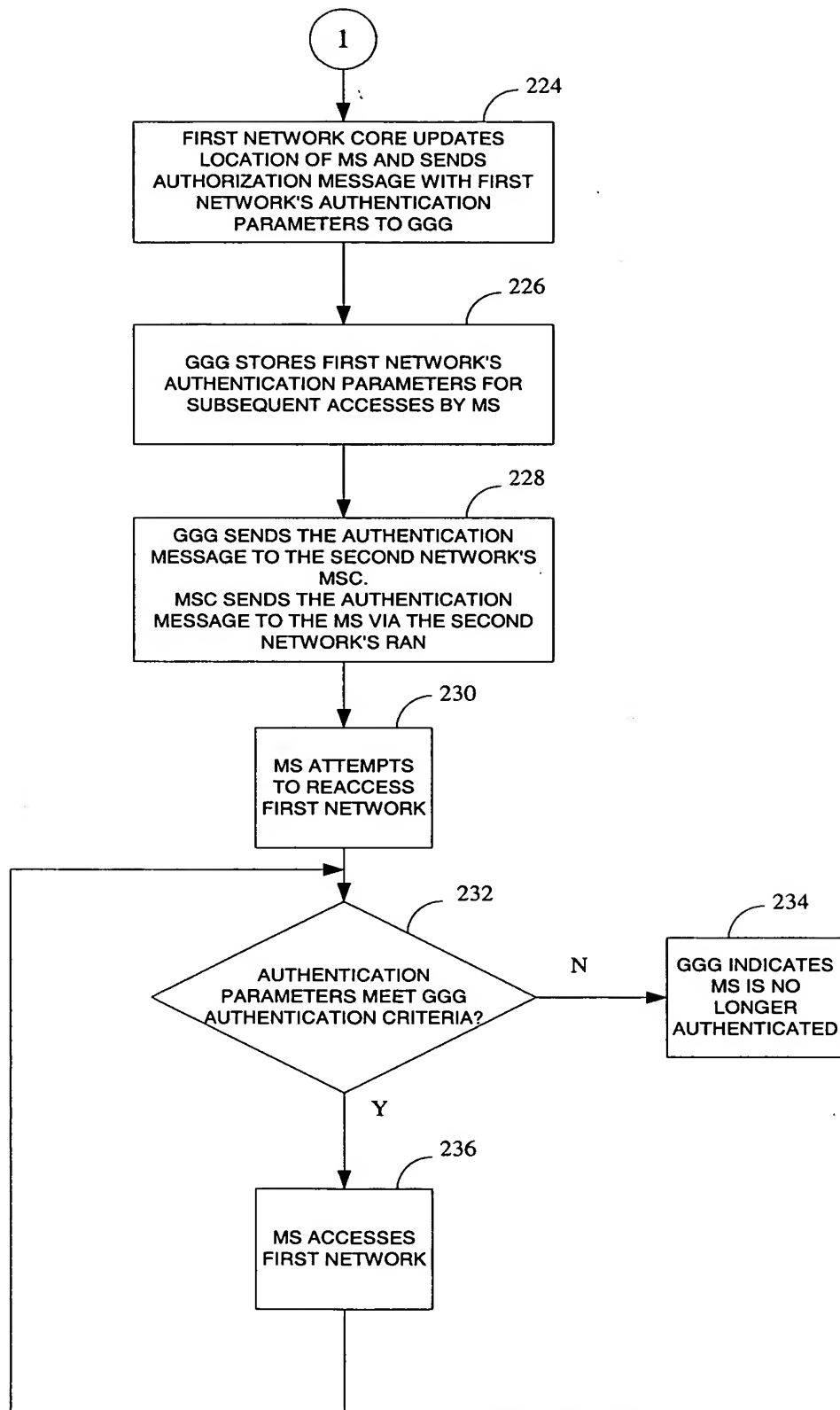
FIGURE 3A

①

224

FIRST NETWORK CORE UPDATES
LOCATION OF MS AND SENDS
AUTHORIZATION MESSAGE WITH FIRST
NETWORK'S AUTHENTICATION
PARAMETERS TO GGG

226

GGG STORES FIRST NETWORK'S
AUTHENTICATION PARAMETERS FOR
SUBSEQUENT ACCESSES BY MS

228

GGG SENDS THE AUTHENTICATION
MESSAGE TO THE SECOND NETWORK'S
MSC.
MSC SENDS THE AUTHENTICATION
MESSAGE TO THE MS VIA THE SECOND
NETWORK'S RAN

230

MS ATTEMPTS
TO REACCESS
FIRST NETWORK

232

AUTHENTICATION
PARAMETERS MEET GGG
AUTHENTICATION CRITERIA?

N → 234

GGG INDICATES
MS IS NO
LONGER
AUTHENTICATED

Y

236

MS ACCESSES
FIRST NETWORK

FIGURE 3B

Figure 4

ANSI-41 method of producing authentication keys
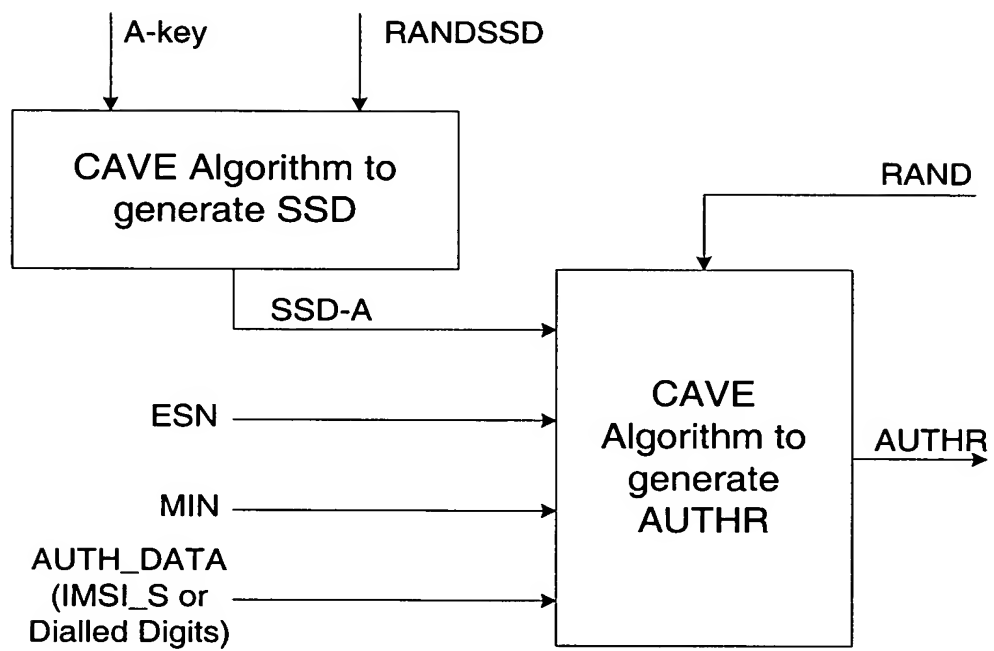
Figure 5

Using Kc as SSD-A
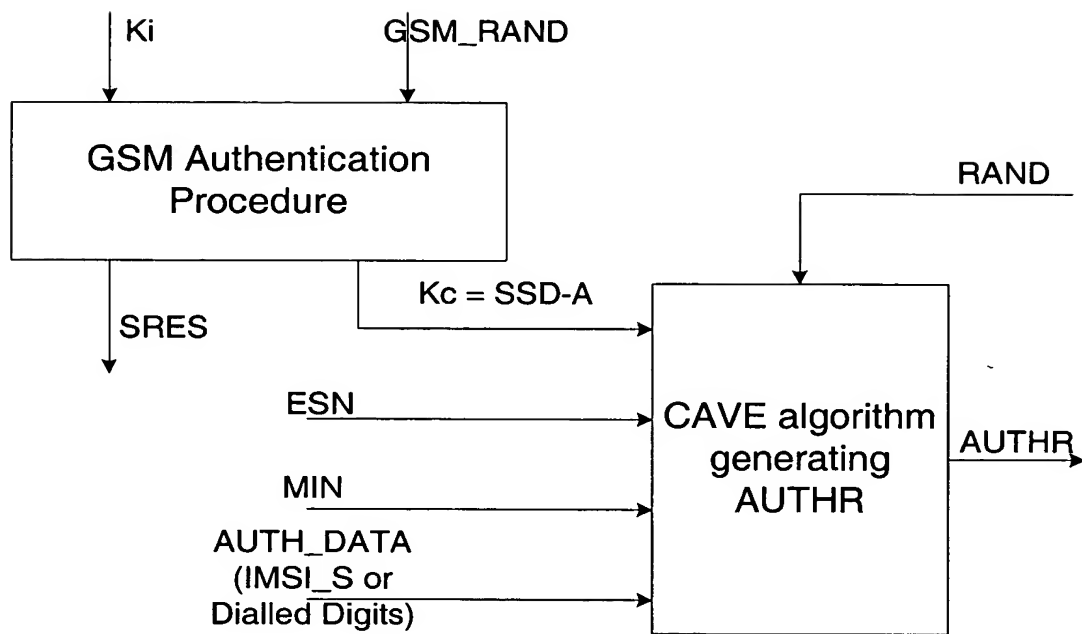
Figure 6

Successful SSD update procedure
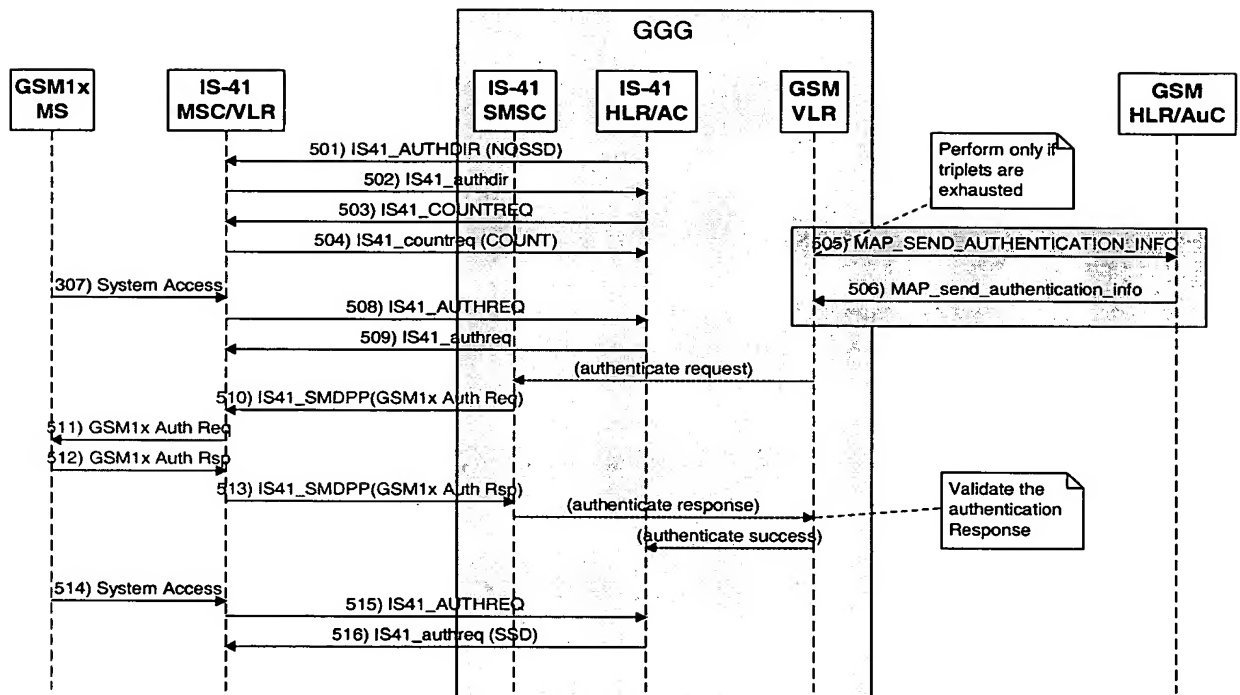
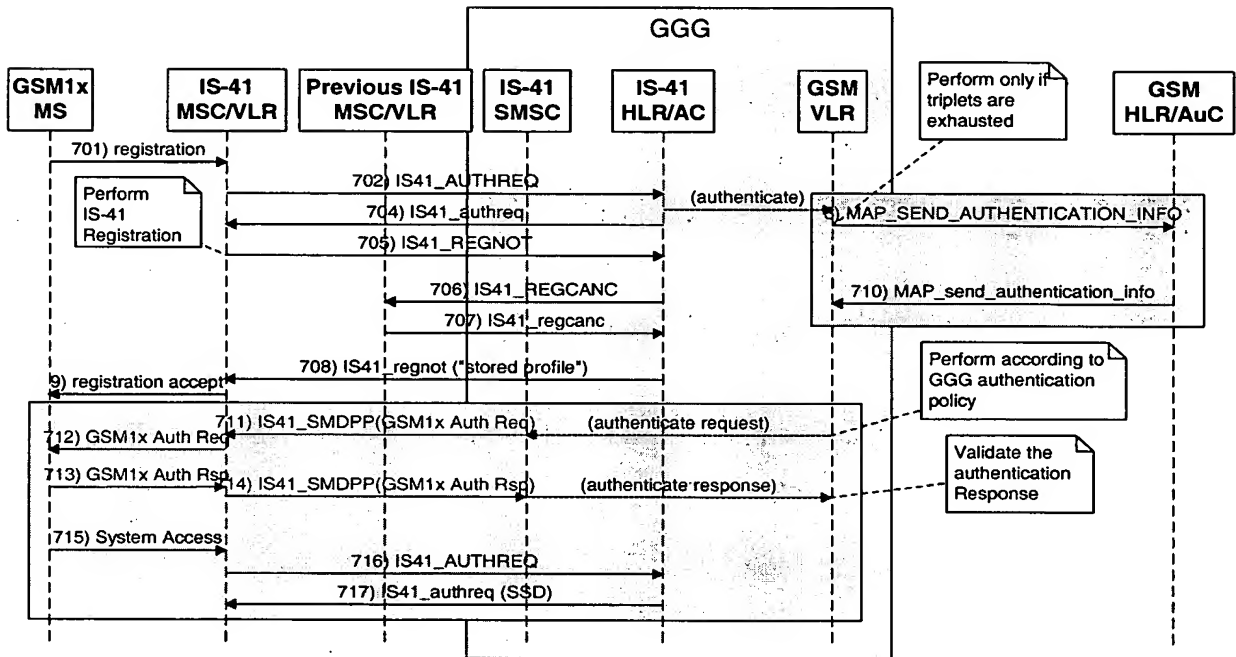# Figure 7

Initial registration with SSD sharing
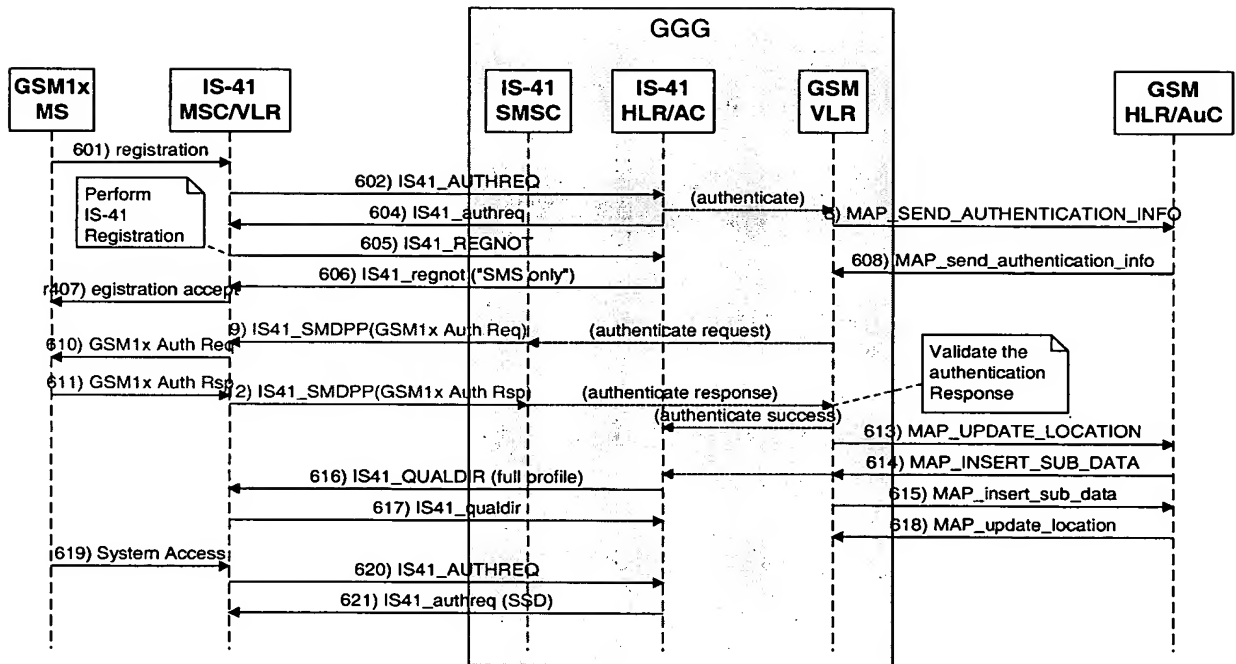
FIGURE 8

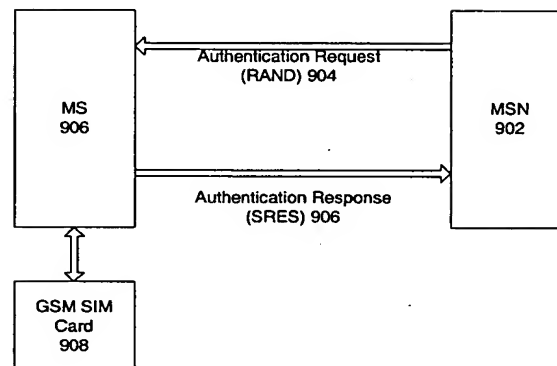## Successful registration with new MSC/VLR with SSD sharing.

Figure 9 - Outline of
Authentication Procedure
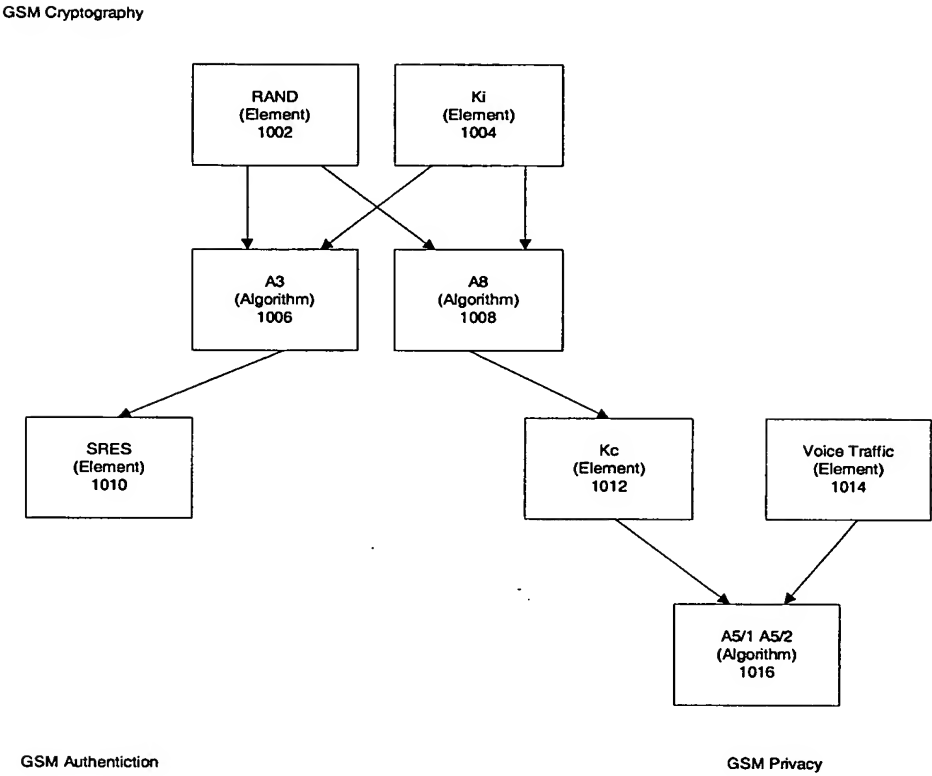
Figure 10 - GSM Key Generation

GSM Cryptography
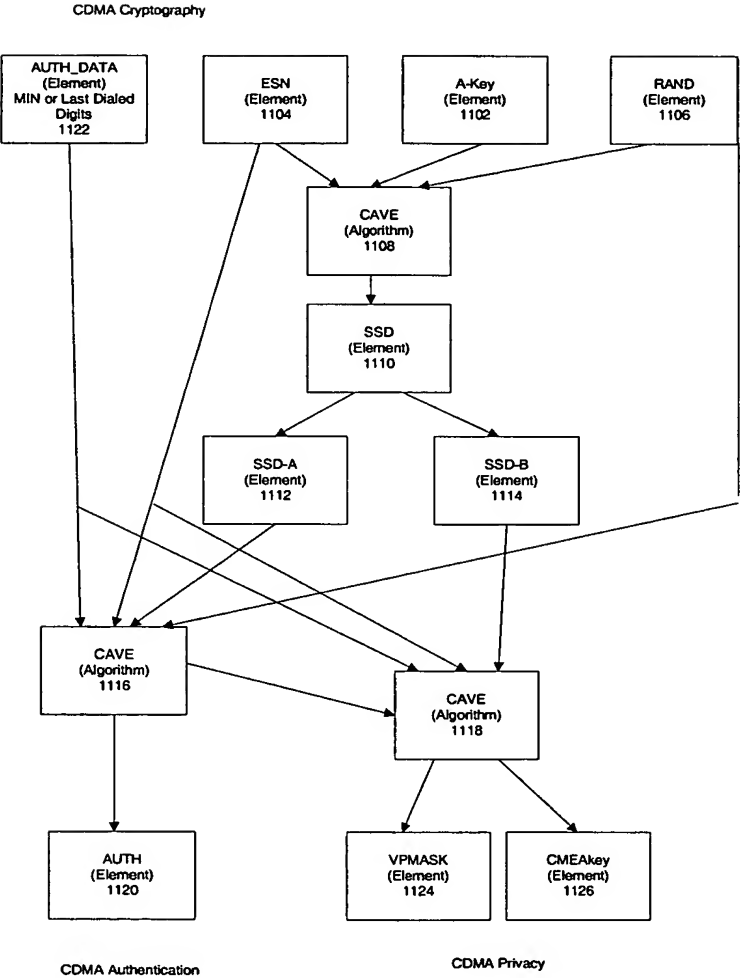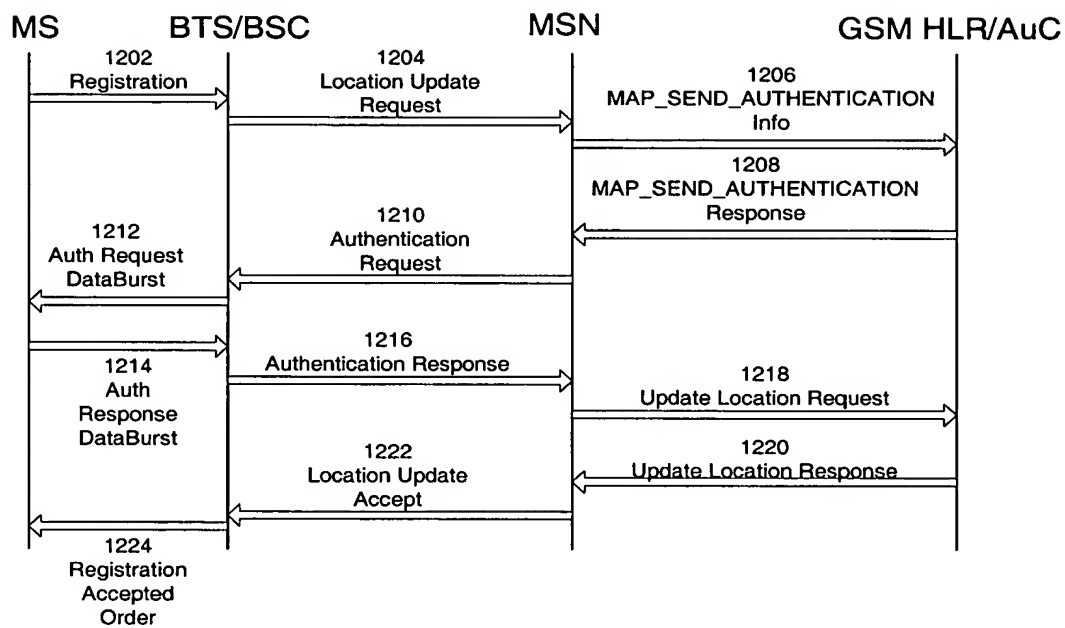

GSM Authentiction   GSM Privacy

Figure 11 - CDMA Key Generation

CDMA Cryptography

CDMA Authentication   CDMA Privacy

Figure 12 - Message Flow during Registration

Figure 13 - Message Flow during MO Call

MS	BTS/BSC	MSN	PSTN

1302
Origination

1306
CM_Service_Request

Ack Order
1304

1308
Assignment Request

1322 IAM

1310
CH Assign

1312
TCH Preamble

1324 ACM

1314
FW Ack Order

1316
Service Connect

1320
Assignment Complete

1318
Service Connect
Complete

Authentication Procedure

Ring Back Tone

1326 ANM

1330
Req Priv Long Code
Transition Order

1328 Privacy Mode

1332
Req Priv Long Code
Transition Resp

1334
Privacy Mode Complete

In Talk State (Scrambled)

Figure 14 - Message Flow during MT Call

MS	BTS/BSC	MSN	PSTN

1402 IAM

1406
General Page

1404 Paging Request

1408
Page Response

1410 Page Response

1414
CH Assign

1412 Assignment Request

1416
TCH Preamble

1418 FW Ack Order

1420 Service Connect

1422 Service Connect
Complete

1426   Assignment Complete

1428 ACM

1424 Alert with
Info

1432   Connect

1430 Connect
Order

Authentication Procedure

1434
Privacy Mode Request

1436
Req Priv Long Code
Transition Order

1440
Privacy Mode Complete

1438
Req Priv Long Code
Transition Resp

1442 ANM

In Talk State (Scrambled)